Primer on Security Patch Management

Objective: Create an environment that is consistently secure from known vulnerabilities in OS and application software where patches are available.

In reality this is impossible. The vulnerability precedes the patch so there is a time delta.

The objective then is to create the ultimate mitigation environment and narrow this gap.

An automated patch management system accompanied by comprehensive patch management policy, standards, baselines and guidelines is recommended.

Most all security appliances, software, methods are accompanied by means of identifying exposure using logs, alerts, etc. Centralized and automated patch management and reporting is essential to understanding exposure and enforcing policy. Development of policy is dependent on the means by which patch management is deployed.

Systems complexity, chains of dependencies, and criticality of operations will, more often than not, necessitate testing of new patches before putting into production.

Systems administrators are chiefly concerned with operational management. Security administrators are chiefly concerned with risk management.

Introducing updates, upgrades, or patches into a production environment has the potential for operational malfunction and compromise of CIA. Likewise, when a vulnerability is publicized, the failure to apply the requisite patch can result in operational malfunction and compromise of CIA. These vulnerabilities can also be used to exploit other connected systems.

Systems and security administrators, alike, are interested in ensuring operational continuity and keeping costs down.

There are government regulations/guidance/policies that advise and/or require systems administrators to apply patches or updates as soon as they are released.

The terms updates, patches, and upgrades are used interchangeably in many of these documents and there are certain regulations, policy, or guidelines that pertain to their installation and administration.

There are primarily four categories of practices under which the installation or administration of updates, patches, or upgrades fall: Configuration Management and Version Control; Change Management; Incident Response; and Disaster Recovery and Business Continuity Planning.

There are requirements and guidelines that can be derived from these practices but they are generally concerned with functionality and operability and not security. There are also some ambiguities amongst the documents that is most likely due to the dating of the material.

Security patching should be enforced though a comprehensive patch management deployment and monitoring program. It should be automated and centralized. Management should be able to, in real-time, know exposure, enable access and instructions to all available patches, and include a means of workflow and accountability during the remediation process.

There are several products on the market that will be the object of evaluation for deployment at FSA. A patch management program will be concurrently developed.